Model theory of difference fields and applications to algebraic dynamics

Zoé Chatzidakis

Abstract. This short paper describes some applications of model theory to problems in algebraic dynamics.

Mathematics Subject Classification (2010). Primary 03C60; Secondary 12H10, 14GXX.

Keywords. Model theory, difference fields, canonical base property.

1. Introduction

A few years ago, Hrushovski noticed that the model theory of difference fields could give a new proof of a result of M. Baker on algebraic dynamics. Baker's result deals with endomorphisms of $\mathbb{P}^1$ defined over a function field K, and shows that under certain conditions, the endomorphism of $\mathbb{P}^1$ is isomorphic (over some algebraic extension of K) to one defined over the constant field k of K. He answered thus a question of Szpiro and Tucker. Nothing was known for varieties of higher dimension. We started working on this together, were able to answer a question of Baker (1.7 in [1]) in case of function fields of characteristic 0, and got a descent result in some special cases: there is a bijective rational map from our original algebraic dynamics (V, ϕ) to one defined over the smaller field. Because our tools are difference fields, the maps we obtain are in general only birational isomorphisms and not isomorphisms when the dimension of the underlying variety is > 1. These results appeared in [4] and [5].

It turns out that another model-theoretic tool, the Canonical Base Property, a property enjoyed by existentially closed difference fields, allows one to obtain a fairly strong result in a more general context. Explaining what is now known is the object of section 4 of this paper.

Section 2 recalls some of the now classical results of the model theory of difference fields, as well as some more recent ones (e.g., 2.12). In section 3, we explain briefly the connection between our algebraic dynamics (V, ϕ) (where ϕ is rational dominant, not necessarily a morphism) and difference fields. In section 4, we introduce the Canonical Base Property, some of its history, give some of its consequences, and explain briefly the strategy to show that existentially closed fields of arbitrary characteristic enjoy it. Section 5 puts everything together.

Proceedings of the International Congress of Mathematicians, Seoul, 2014

2. Difference fields and their model theory

2.1. Basic definitions. A difference ring is a ring R with a distinguished endomorphism σ. A *difference* field is a difference ring which is a field (note that the endomorphism will necessarily be injective). A difference ring becomes naturally a structure of the language $\mathcal{L} = \{+, -, \cdot, \sigma, 0, 1\}$, where $+, -, \cdot$ are interpreted as the usual binary operations, 0 and 1 are the usual constants, and σ is interpreted by the endomorphism. The difference ring is *inversive* if the endomorphism is onto. Every difference ring R has a unique up to R-isorphism *inversive closure*, or *inversive hull*, i.e., an inversive difference ring containing it, and which R-embeds into every inversive difference field containing R.

The *difference polynomial ring in the variables* $Y = (Y_1, \ldots, Y_n)$ *over* R, denoted $R[Y]_\sigma$, is the polynomial ring $R[\sigma^j(Y_i) \mid 1 \leq i \leq n, j \geq 0]$, endowed with the natural extension of σ defined by sending $\sigma^j(Y_i)$ to $\sigma^{j+1}(Y_i)$ for each i and j.

If K is a field, then zero-sets of elements of $K[Y_1, \ldots, Y_n]_\sigma$ generate the closed sets of a topology on K^n, and this topology is Noetherian. It is very similar to the Zariski topology. I will call the closed sets of this topology *σ-closed.*

All these results and more can be found in Richard Cohn's book [7].

2.2. The model theory of existentially closed difference fields. A difference field K is *existentially closed* if every finite system of difference equations with coefficients in K which has a solution in a difference field containing K, has a solution in K. Note that an existentially closed difference field is necessarily inversive and algebraically closed. Every difference field embeds into an existentially closed one, and the existentially closed difference fields form an elementary class, with theory usually called ACFA. These fields were first investigated in the 90's by Macintyre, Van den Dries and Wood, see [12]. An indepth study, concentrating on geometric stability properties of these fields was then started by Hrushovski and myself, later joined by Peterzil [3, 6]. I will now recall some of the classical results.

The theory ACFA expresses the following properties of the $\mathcal{L}$-structure K:

– K is algebraically closed, $\sigma \in \mathrm{Aut}(K)$;

– If U, V are irreducible (algebraic) varieties, with $U \subset V \times V^\sigma$, and such that U projects dominantly onto V and V^σ, then there is a such that $(a, \sigma(a)) \in U$. [Here V^σ denotes the variety obtained by applying σ to the defining equations of V.]

2.3. Notation. $\mathbb{N}$ denotes the set of non-negative integers. We will work in a large sufficiently saturated existentially closed difference field $\mathcal{U}$. If E is a field, then E^{alg} denotes the (field-theoretic) algebraic closure of E. If E is a difference subfield of $\mathcal{U}$, and a a tuple in $\mathcal{U}$, then $E(a)_\sigma$ denotes the difference field generated by a over E, i.e. $E(a)_\sigma = E(\sigma^i(a) \mid i \in \mathbb{N})$, and $E(a)_{\sigma^{\pm 1}}$ its inversive hull $E(a)_{\sigma^{\pm 1}} = E(\sigma^i(a) \mid i \in \mathbb{Z})$.

2.4. Some properties of ACFA and of its models. Most of the results here appear in [13] or in [3]. ACFA does not eliminate quantifiers, the problem coming from the fact that an automorphism of a field E needs not extend uniquely to the algebraic closure E^{alg} of E. However, this is the only obstacle, and one obtains that if E is an algebraically closed difference field, then ACFA $\cup\, \mathrm{qfDiag}(E)$ is complete (Here $\mathrm{qfDiag}(E)$ denotes the quantifier-free diagramme of E in the language $\mathcal{L}(E)$ obtained by adjoining constant symbols for the elements of E). This last result has several important consequences:

(1) Completions of ACFA are obtained by describing the action of the automorphism on

the algebraic closure of the prime field. This implies that ACFA is decidable.

(2) If E is a difference subfield of a model $\mathcal{U}$ of ACFA, and a, b are tuples in $\mathcal{U}$, then $tp(a/E) = tp(b/E)$ if and only if there is an E-isomorphism $E(a)_\sigma^{alg} \to E(b)_\sigma^{alg}$ which sends a to b.

(3) If $A \subset \mathcal{U}$, then the model-theoretic algebraic closure $\mathrm{acl}(A)$ of A is the smallest inversive algebraically difference field containing A. The definable closure of A, $\mathrm{dcl}(A)$, is usually much larger than the inversive difference field generated by A: it is the subfield of $\mathrm{acl}(A)$ fixed by the elements of $\mathrm{Aut}(\mathrm{acl}(A)/A)$ which commute with σ.

(4) Let $S \subset \mathcal{U}^n$ be definable. Then there is a set $W \subset \mathcal{U}^{n+m}$ defined by difference equations such that the projection π on the first n coordinates defines a finite-to-one map from W onto S.

One can also show that any completion of the theory ACFA is supersimple (of SU-rank ω), and that it eliminates imaginaries. An important definable subset of $\mathcal{U}$, is the *fixed field*

$$\mathrm{Fix}(\sigma) := \{a \in \mathcal{U} \mid \sigma(a) = a\}.$$

It is a pseudo-finite field, and its induced structure is that of a pure field. It is also stably embedded, and therefore, if $S \subset \mathrm{Fix}(\sigma)^n$ is definable in $\mathcal{U}$ with parameters from $\mathcal{U}$, then it is of the form $S' \cap \mathrm{Fix}(\sigma)^n$, where S' is definable in the langauge of rings with parameters from $\mathrm{Fix}(\sigma)$.

In positive characteristic p, there are other definable automorphisms, which are built up using the definable Frobenius automorphism $\mathrm{Frob} : x \mapsto x^p$ and its powers Frob_q. More precisely, if $\tau = \sigma^n \mathrm{Frob}^m$, where $n \geq 1$, $m \in \mathbb{Z}$, then $\mathrm{Fix}(\tau)$ is a pseudo-finite field, stably embedded; the induced structure is that of a pure field if $n = 1$, but involves the automorphism σ if $n > 1$. We will also call $\mathrm{Fix}(\tau)$ a fixed field. One has the following result:
(1.12 in [3]) *Let τ be as above, (K, σ) a model of ACFA, and consider its reduct the difference field (K, τ). Then $(K, \tau) \models$ ACFA.*

2.5. Independence and SU-rank. As the theory is supersimple, every type is ranked by the rank SU, a rank based on forking (or non-independence). In what follows, A, B, C are subsets of $\mathcal{U}$, a is a tuple of elements of $\mathcal{U}$, and E is a difference subfield of $\mathcal{U}$.

Independence of A and B over C, denoted $A \mathop{\smile\!\!\!\!\!\mid}_C B$, is characterized by the linear disjointness of the fields $\mathrm{acl}(CA)$ and $\mathrm{acl}(CB)$ over $\mathrm{acl}(C)$. A set D definable over E has finite SU-rank iff every tuple $a \in D$ has finite SU-rank over E, and then

$$\mathrm{SU}(D) = \sup\{\mathrm{SU}(a/E) \mid a \in D\}.$$

One shows easily the following:

- $\mathrm{SU}(a/E) = 0$ if and only if $a \in \mathrm{acl}(E)$.
- $\mathrm{SU}(a/E) \leq 1$ if and only if for every $B \supset E$, either a and B are independent over E, or $a \in \mathrm{acl}(B)$.
- If $\mathrm{tr.deg}(E(a)_\sigma/E) < \infty$, and F is a difference field containing E, then $a \mathop{\smile\!\!\!\!\!\mid}_E F$ if and only if $\mathrm{tr.deg}(E(a)_\sigma/E) = \mathrm{tr.deg}(F(a)_\sigma/F)$.
- If $\mathrm{tr.deg}(E(a)_\sigma/E) < \infty$, then $\mathrm{SU}(a/E) \leq \mathrm{tr.deg}(E(a)_\sigma/E)$.

- $\mathrm{SU}(a/E) < \omega$ if and only if $\mathrm{tr.deg}(E(a)_\sigma/E) < \infty$.

If $\mathrm{SU}(a/E) < \omega$, then $tp(a/E)$ can be *analysed* in terms of types of SU-rank 1, and so types of SU-rank 1 determine the properties of $tp(a/E)$. This will be explained below in the paragraph on semi-minimal analyses. First, a few definitions:

Definition 2.6. Let T be a supersimple theory which eliminates imaginaries, $\mathbb{U}$ a sufficiently saturated model of T, and $S \subset \mathbb{U}^n$, $P \subset \mathbb{U}^m$ subsets which are invariant under $\mathrm{Aut}(\mathbb{U}/A)$ for some small subset A of $\mathbb{U}$. E.g. S is A-definable, or is a union of realisations of types over A.

(1) S is *one-based* if whenever $a_1,\dots,a_\ell \in S$ and $B \supset A$, $C = \mathrm{acl}(Aa_1\dots,a_\ell)\cap\mathrm{acl}(AB)$, then $(a_1,\dots,a_\ell)$ and B are independent over C.

(2) A partial type is *one-based* if the set of its realisations is one-based.

(3) S is *internal to* P, resp. *almost-internal to* P, if for some finite set B, we have $S \subset \mathrm{dcl}(ABP)$, resp. $S \subset \mathrm{acl}(ABP)$.

(4) (difference field context) S is *qf-internal to* P if for some finite set B, if $a \in S$, then there is some tuple b of elements of P such that a is in the inversive difference field generated by ABb.

(5) If p, q are types, we say that p is internal, almost-internal, qf-internal, to q, if the set of realisations of p is internal, almost-internal, qf-internal, to the set of realisations of q.

The following is one of the major results in the model theory of difference fields, and is often called the *dichotomy theorem*:

Theorem 2.7 ([3, 6]). *Let q be a type of SU-rank 1 in a model $\mathcal{U}$ of ACFA. Then either q is one-based, or it is almost internal*[1] *to the generic type of* $\mathrm{Fix}(\tau)$, *where $\tau = \sigma$ if the characteristic is 0, and in positive characteristic, τ is of the form $\sigma^n\mathrm{Frob}^m$ for some $n \geq 1$, $m \in \mathbb{Z}$ relatively prime to n. Moreover, if the characteristic is 0 and q is one-based, then q is stable stably embedded.*

So, Theorem 2.7 tells us that if a type of SU-rank 1 is not one-based, then it is almost internal to $\mathrm{Fix}(\tau)$ for some definable τ. The property of being one-based is very strong, since it gives a criterion for independence. It also forbids the existence of two distinct group laws, such as in fields. Hrushovski and Pillay ([11]) showed that stable one-based groups of finite rank are particularly nice, and their result generalises partially to our context, as follows:

Theorem 2.8. *Let G be an algebraic group definable in a model $\mathcal{U}$ of ACFA, et let B be a quantifier-free definable subgroup of $G(\mathcal{U})$ which is one-based, and defined over some $E = \mathrm{acl}(E)$. Let X be a quantifier-free definable subset of B^n. Then X is a Boolean combination of cosets of E-definable subgroups of B^n.*

In particular, if Y is a subvariety of G^n, then $Y \cap B^n$ is a finite union of translates of quantifier-free definable subgroups of B^n.

If $\mathcal{U}$ has characteristic 0, the result extends to arbitrary definable group G and definable subsets X of B^n: they are Boolean combination of translates of definable subgroups of B^n, and these subgroups are defined over E.

[1]The original formulation is: non-orthogonal to

The following gives a useful characterization of types of SU-rank 1 which are almost-internal to $\mathrm{Fix}(\sigma)$:

Theorem 2.9. *Let $\mathcal{U}$ be a model of ACFA, $E = \mathrm{acl}(E)$ a difference subfield of $\mathcal{U}$ and b a tuple in $\mathcal{U}$, with SU$(b/E) = 1$. Then $tp(b/E)$ is almost-internal to the generic type of $\mathrm{Fix}(\sigma)$ if and only if*

$$\mathrm{tr.deg}(E(b)_\sigma/E) = 1 \textit{ and } \{[E(b, \sigma^\ell(b)) : E(b)] \mid \ell \in \mathbb{Z}\} \textit{ is bounded.}$$

2.10. Some consequences of the dichotomy. The fact that definable sets which are orthogonal to the fixed fields are one-based, is at the core of several applications to number theory, by Hrushovski ([9]) and by Scanlon ([17–19]). I will explain how its use gives a new proof of the conjecture of Manin-Mumford. Recall first the

Conjecture of Manin-Mumford. *Let A be an abelian variety defined over a number field k, and let $X \subset A$ be a subvariety. Then the Zariski closure of $X(k^{alg}) \cap \mathrm{Tor}(A)(k^{alg})$ is a finite union of translates of abelian subvarieties of A by torsion points.*

This conjecture, as well as several strengthenings (A a commutative algebraic group, k an arbitrary field, with similar conclusions) have been proved using different methods. The one by Hrushovski deals with an arbitrary commutative algebraic group G defined over a number field. One important point is that the torsion subgroup lives in the semi-abelian quotient of the group, and he shows that the number of components of the Zariski closure of $\mathrm{Tor}(G) \cap X$ is bounded by the number of components of the Zariski closure of $\mathrm{Tor}(H) \cap \pi(X)$, where H is the quotient of G by its maximal vector subgroup, and $\pi : G \to H$ is the natural map. Results of Mumford, together with a characterization by Hrushovski of one-based subgroups of abelian varieties or of $\mathbb{G}_m$, allow him to show that there is some $\sigma \in \mathrm{Aut}(\mathbb{Q})$ such that the torsion subgroup of G is contained in a quantifier-free definable subgroup B of G, which defines a one-based group in any existentially closed difference field containing $(\bar{\mathbb{Q}}, \sigma)$. This, together with 2.8 and a simple argument, give the result. Bounds on the complexity of the difference equations defining B give bounds on the number of cosets involved in the description.

The applications by Scanlon have a similar flavour.

2.11. The classical semi-minimal analysis. A standard result on supersimple theories states that if $tp(a/E)$ has finite SU-rank, then there are SU-rank 1 types $p_1, \dots, p_n$, and tuples $a_1, \dots, a_n$ such that $\mathrm{acl}(Ea) = \mathrm{acl}(Ea_1 \dots, a_n)$, and for each i, $tp(a_i/Ea_{i-1})$ is almost-internal to p_i. Such a sequence $a_1, \dots, a_n$ is called a *semi-minimal analysis of* $tp(a/E)$.

It may happen that one can choose the a_i's such that each $tp(a_i/E)$ is almost-internal to p_i; in that case, notice that $tp(a/E)$ is almost internal to the set S of realisations of the p_i's. This is a strong condition on $tp(a/E)$, and we will say in this case that $tp(a/E)$ is *almost-internal* [to types of rank 1].

One can refine the semi-minimal analysis a little and impose that the a_i's are in $\mathrm{dcl}(Ea)$, and that the types $tp(a_i/\mathrm{acl}(Ea_{i-1}))$ are internal to p_i, for all i. But, as mentioned above, in the case of difference fields, the definable closure is too large to hope obtain precise results on definable sets. After some work, and precise analysis of what internality to a fixed field means, one obtains the following result:

Proposition 2.12 ([5, 2.13]). *Let E be an inversive difference field, a a tuple in $\mathcal{U}$ such that $\sigma(a) \in E(a)^{alg}$.*

(1) *Then there are $a_1, \dots, a_n = a \in E(a)_\sigma$, such that, setting $A_i = E(a_{i-1})_\sigma$ for each i (with $a_0 = \emptyset$), $tp(a_i/A_i)$ satisfies one of the following:*

  (i) *$tp(a_i/A_i)$ is algebraic;*
  (ii) *$tp(a_i/A_i)$ is one-based;*
  (iii) *$tp(a_i/A_i)$ is qf-internal to $\mathrm{Fix}(\tau)$ for some $\tau = \mathrm{Frob}^m \sigma^n$.*

(2) *Furthermore, let $\ell \geq 1$ be an integer, $(\mathcal{U}', \sigma')$ a model of ACFA, and $f : (E(a)_\sigma, \sigma^\ell) \to (\mathcal{U}', \sigma')$ an embedding of difference fields. Then, if $a_1, \dots, a_n$ are as in (1), we have similar results holding in $\mathcal{U}'$: $tp^{\mathcal{U}'}(f(a_i)/f(A_i))$ is algebraic in case* (i)*, one-based in case* (ii)*, and qf-internal to $\mathrm{Fix}(\tau^\ell)$ in case* (iii).

The content of this proposition is very strong. Note that in particular it implies that whether the tuple a is "one-based over E" depends only on its quantifier-free type over E, not on the particular embedding of $E(a)_\sigma$ into a model of ACFA. This result decomposes the extension $E(a)_\sigma/E$ into a tower of field extensions, each one of a certain kind.

3. Difference fields and algebraic dynamics

Definition 3.1. An *algebraic dynamics* defined over a field K is given by a pair (V, ϕ) consisting of a (quasi-projective) variety defined over K, together with a rational dominant map $\phi : V \to V$.

Remarks 3.2. In the literature, ϕ is often assumed in addition to be a morphism. Moreover, one also often imposes that the morphism be *polarized*, i.e., that there is an ample vector bundle $\mathfrak{L}$ on V and an integer $q > 1$ such that $\phi^* \mathfrak{L} \simeq \mathfrak{L}^{\otimes q}$. These hypotheses have strong consequences which we will discuss later.
If L is a field extension of K, an algebraic dynamics (V, ϕ) gives naturally rise to one defined over L, by viewing V as defined over L. We will constantly use this remark, and always consider them as algebraic dynamics over a large ambient algebraically closed field $\mathcal{U}$ (while they may be defined over smaller subfields).
If V is not absolutely irreducible, it may become reducible when viewed over L, and for this reason **we will always assume that our varieties are absolutely irreducible**.

Definition 3.3. If (V, ϕ) and (W, ψ) are algebraic dynamics, a *morphism* $(V, \phi) \to (W, \psi)$ is a rational map $f : V \to W$ such that $f \circ \phi = \psi \circ f$. It is *dominant* if $f : V \to W$ is dominant.

(3.4) Let (V, ϕ) be as above, and consider the function field $K(V)$ of V. The map ϕ then yields an endomorphism ϕ^* of $K(V)$, which leaves K fixed, and is defined by $f \mapsto f \circ \phi$, for $\phi \in K(V)$ (We view the elements of $K(V)$ as partial functions on $V(K)$ taking their values in K).
The *degree* of the morphism ϕ is $\deg(\phi) = [K(V) : \phi^* K(V)]$

Another equivalent way of translating algebraic dynamics into the difference field context, is the following: let a be a generic of V over K, and define an endomorphism σ of $K(a)$ by letting σ be the identity on K, and setting $\sigma(a) = \phi(a)$. If $f : (V, \phi) \to (W, \psi)$ is a dominant morphism, then $b = f(a)$ will be a generic of W, and we will have $\sigma(b) = \psi(b)$. Thus dominant morphisms of algebraic dynamics correspond to inclusions of difference fields.

3.5. Applying the semi-minimal analysis. Applying 2.12, there are tuples $a_1, \ldots, a_n = a \in K(a)$, such that for each i, $\sigma(a_i) \in K(a_i) \subset K(a_{i+1})$, and $tp(a_i/K(a_{i-1}))$ is either algebraic, or qf-internal to $\mathrm{Fix}(\tau)$, or one-based.

These tuples a_i give rise to a fibration of (V, ϕ), namely, if V_i is the algebraic locus of a_i over K, ϕ_i the rational endomorphism of V_i such that $\sigma(a_i) = \phi_i(a_i)$ and $g_i : V_i \to V_{i-1}$ the rational map induced by the inclusion $K(a_{i-1}) \subset K(a_i)$, we obtain

$$(V, \phi) \xrightarrow{g_n} (V_{n-1}, \phi_{n-1}) \xrightarrow{g_{n-1}} \cdots \xrightarrow{g_2} (V_1, \phi_1).$$

Note that the fibers of these maps are not themselves algebraic dynamics: indeed, the map σ transports the fiber $f_n^{-1}(a_{n-1})$ to $f_n^{-1}(\sigma(a_{n-1})) = f_n^{-1}(\phi_{n-1}(a_{n-1}))$.

3.6. Internality to the fixed field $\mathrm{Fix}(\boldsymbol{\sigma})$. Assume that $tp(a_i/K(a_{i-1}))$ is internal to $\mathrm{Fix}(\sigma)$, and that $K(a_i)$ intersects the separable closure $K(a_{i-1})^s$ of $K(a_{i-1})$ in $K(a_{i-1})$. Then, over some L containing $K(a_{i-1})$ and linearly disjoint from $K(a_i)$ over $K(a_{i-1})$, there is a tuple b such that $L(a_i) = L(b)$ and $\sigma(b) = b$. This implies that $L(a_i) = L(\sigma(a_i))$. If $i = 1$, then we get that ϕ_1 is a birational map, i.e., has degree 1. If $i \geq 2$, we obtain that ϕ_i induces a birational map between $g_i^{-1}(a_{i-1})$ and $g_i^{-1}(\sigma(a_{i-1}))$, and we have $\deg(\phi_i) = \deg(\phi_{i-1})$.

3.7. Algebraic extensions. Note that if a_j is algebraic over $K(a_{j-1})$, then also $\deg(\phi_j) = \deg(\phi_{j-1})$.

4. The Canonical base property

This property was originally a property of compact complex manifolds, which was isolated (independently) by Campana and Fujiki. Work of Moosa and Pillay provided a translation of this property in model-theoretic terms ([13] and [15]); Pillay and Ziegler ([16]) showed that various enriched fields enjoy it. This property will be later called the Canonical Base Property, CBP for short, by Moosa and Pillay who investigate it further in [14], and ask several questions.

Definition 4.1. Let T be a theory which eliminates imaginaries, $\mathbb{U}$ a saturated model of T, $A \subset \mathbb{U}$ and a a tuple in $\mathbb{U}$, $p(x) = tp(a/A)$.

(1) If T is stable and p is stationary, then p is definable, that it, for every formula $\varphi(x, y)$, there is a formula $d_\varphi(y)$ (with parameters in A) such that for every tuple b in A (of the correct arity), $\mathbb{U} \models d_\varphi(b)$ if and only if $\varphi(x, b) \in p$. Furthermore, these definitions define a (consistent and complete) type over $\mathbb{U}$. The *canonical base* of p is the smallest definably closed subset of $\mathcal{U}$ over which one can find parameters for all the formulas $d_\varphi(y)$ (in other words, contains the code of all sets defined by the $d_\varphi(y)$). It is denoted by $\mathrm{Cb}(p)$ or $\mathrm{Cb}(a/A)$, and is contained in A.

(2) If T is unstable, but simple, then the definition of canonical base is more involved, see e.g. Wagner's book [20], as it is defined in terms of extension base. It is easier to define the algebraic closure of the canonical base, denoted $\overline{\mathrm{Cb}}(p)$ or $\overline{\mathrm{Cb}}(a/A)$: it is the smallest algebraically closed subset B of A such that a and A are independent over B. If T is supersimple, then $\overline{\mathrm{Cb}}(p)$ will be contained in the algebraic closure of finitely many realisations of p, and so will have finite SU-rank if p has. Note that this definition also makes sense for infinite tuples, and we will often use it for the infinite tuple enumerating the algebraic closure of a finite tuple.

Example 4.2. Consider the theory ACF of algebraically closed fields, say of characteristic 0 for simplicity, and let $\mathbb{U}$ be a large algebraically closed field, $A \subset \mathbb{U}$ a subfield, and a a tuple in $\mathbb{U}$. Assume that $A(a)$ is a regular extension of A, and consider the algebraic locus V of a over A. Then $\mathrm{Cb}(a/A)$ is simply the field of definition of V.

Example 4.3. Let a be a tuple in $\mathcal{U}$, E a difference subfield of $\mathcal{U}$. If X is a tuple of indeterminates of the same size as a, then one can consider the ideal I of $E[X]_\sigma$ of difference polynomials which vanish at a. As in classical geometry, this ideal has a smallest (difference) field of definition, i.e., there is a unique smallest difference subfield E_0 of E such that I is generated by its intersection with $E_0[X]_\sigma$. Then $\overline{\mathrm{Cb}}(a/E) = \mathrm{acl}(E_0)$.

Definition 4.4. Let T be a supersimple theory which eliminates imaginaries. We say that T has the *Canonical Base Property*, or *CBP*, if whenever A and B are algebraically closed sets such that $\mathrm{SU}(A/A \cap B) < \omega$ and $B = \overline{\mathrm{Cb}}(A/B)$, then $tp(B/A)$ is almost-internal (to types of SU-rank 1).

4.5. Comments.

(1) Let $C = A \cap B$, and a, b finite tuples such that $A = \mathrm{acl}(Ca)$, $B = \mathrm{acl}(Cb)$. Then $\mathrm{SU}(A/C) = \mathrm{SU}(a/C)$. The notion of almost-internality is by definition preserved under passage to the algebraic closure, so there are a set $D = \mathrm{acl}(D)$ containing A and independent from B over A, and tuples $b_1, \dots, b_n$ with $\mathrm{SU}(b_i/D) = 1$, such that $\mathrm{acl}(DB) = \mathrm{acl}(Db_1 \dots b_n)$.

(2) The definition in the stable case deals with finite tuples a and b, assumes that $\mathrm{Cb}(a/b)$ $= b$, and deduces that $tp(b/a)$ is internal to types of rank 1.

(3) If $tp(A/C)$ is one-based, then ... by definition of one-basedness, we know that A and B are independent over their intersection, and therefore $B = C$. To say it in another fashion: if $tp(a/E)$ is one-based, and B contains E, then $\overline{\mathrm{Cb}}(a/B) \subset \mathrm{acl}(Ea)$.

(4) Hrushovski, Palacin and Pillay give in [10] an example of an ω-stable theory of finite rank which does not have the CBP. This example is built up from the theory ACF of algebraically closed fields.

Theorem 4.6 (Pillay-Ziegler [16]).

(1) *The theory of differentially closed fields of characteristic* 0 *has the CBP* (*version for stable theories*).

(2) *The elementary theory of an existentially closed difference field of characteristic* 0 *has the CBP.*

Pillay and Ziegler have some additional partial results concerning types of rank 1 in separably closed fields, but not the full and hoped for result. Their proof uses jet spaces, and generalises only partially to positive characteristic, because of possible inseparability problems. In order to show that the result holds for existentially closed fields of arbitrary characteristic, one needs to show a decomposition result:

Theorem 4.7 (1.16 in [2]). *Let T be a supersimple theory, $\mathbb{U}$ a large model of T, A, B and $C = A \cap B$ algebraically closed subsets of $\mathbb{U}$ such that $\mathrm{SU}(A/C) < \omega$ and $B = \overline{\mathrm{Cb}}(A/B)$. Then there are $a_1, \dots, a_n \in A$, types $p_1, \dots, p_n$ of SU-rank 1 (maybe over some larger base set D which is independent from AB over C), such that $\mathrm{acl}(Ca_1 \dots, a_n) = \mathrm{acl}(CA)$; and each $tp(a_i/C)$ has a semi-minimal analysis in which all components are almost-internal to the set of realisations of the $\mathrm{Aut}(\mathbb{U}/C)$-conjugates of p_i.*
Furthermore, each of the types p_i is non-one-based.

From this, one shows easily that it suffices to show the CBP for types whose semi-minimal analysis only involves one fixed non-one-based type of rank 1. In the particular case of existentially closed difference fields of positive characteristic p, we must therefore look at types analysable in terms of $\mathrm{Fix}(\tau)$, for the various possible τ. When $\tau = \sigma$, one shows the following:

Lemma 4.8. *Let a be a finite tuple in $\mathcal{U}$, of finite SU-rank over $E = \mathrm{acl}(E)$, and assume that the semi-minimal analysis of $tp(a/E)$ only involves $\mathrm{Fix}(\sigma)$-almost-internal types. Then there is a tuple $b \in E(a)_{\sigma^{\pm 1}}$ such that $E(a)_{\sigma^{\pm 1}}$ is separably algebraic over $E(b)$.*

Inspection of the proof of Pillay-Ziegler then shows that there is no problem when $\tau = \sigma$: their proof goes through verbatim. Working in the reduct $(\mathcal{U}, \tau)$ then allows to obtain the results for all types analysable in $\mathrm{Fix}(\tau)$. Using the dichotomy Theorem 2.7, this finishes the proof of

Theorem 4.9 (3.5 in [2]). *Existentially closed difference fields of any characteristic have the CBP.*

The CBP has several interesting consquences, which I will now list. Relative versions of these results exist.

Theorem 4.10 (References are to [2]). *Let T be a supersimple theory with the CBP, $\mathbb{U}$ a saturated model, and $A, B, C = A \cap B$ algebraically closed subsets of $\mathbb{U}$, with $\mathrm{SU}(A/C)$ finite.*

(1) (2.1) *If $B = \overline{\mathrm{Cb}}(A/B)$, then $tp(B/C)$ is almost-internal.*

(2) (2.2) *More generally, if $tp(B/A)$ is almost-internal, then so is $tp(B/C)$.*

(3) (2.4) *There is some $D = \mathrm{acl}(D)$ with $C \subseteq D \subseteq A$ such that whenever $E = \mathrm{acl}(E)$ is such that $tp(A/E)$ is almost-internal, then $E \subseteq D$.*

(4) (2.5) *If $B = \overline{\mathrm{Cb}}(A/B)$ and D is such that $tp(A/D)$ is almost-internal, then so is $tp(AB/D)$.*

(5) (2.10) *Let a_1, a_2, b_1, b_2 be tuples of finite SU-rank, $\mathcal{S}$ a set of types of SU-rank 1 and assume that*

– *$tp(b_2)$ is almost-internal to types in $\mathcal{S}$,*

– $\mathrm{acl}(b_1) \cap \mathrm{acl}(b_2) = \mathrm{acl}(\emptyset)$,

– $a_1 \perp_{b_1} b_2$ *and* $a_2 \perp_{b_2} b_1$,

– $a_2 \in \mathrm{acl}(a_1 b_1 b_2)$.

Then there is $e \subset \mathrm{dcl}(a_2 b_2)$ *such that* $tp(a_2/e)$ *is almost-internal to types in* $\mathcal{S}$ *and* $e \perp b_2$. *In particular, if* $tp(a_2/b_2)$ *is hereditarily orthogonal to all types in* $\mathcal{S}$, *then* $a_2 \in \mathrm{acl}(e b_2)$.

4.11. Comments. Here is an easy consequence of item (1): assume that $tp(A/C)$ is not almost-internal, has finite SU-rank, and that $A \cap B = C$. Then A and B are independent over C.
Item (4) answers a question of Moosa and Pillay ([14]).
Item (5) is a *descent result*, and is (together with 2.12) the main ingredient of the applications to algebraic dynamics by Hrushovski and myself. After some work, and use of Proposition 2.12, one refines the descent result 4.10(5) to obtain the following:

Theorem 4.12 (4.11 in [2]). *Let* K_1, K_2 *be fields intersecting in* k, *for* $i = 1, 2$, *and with algebraic closures intersecting in* k^{alg}, *let* V_i *be an absolutely irreducible variety and* $\phi_i : V_i \to V_i$ *a dominant rational map defined over* K_i. *Assume that* K_2 *is a regular extension of k, and that there is an integer* $r \geq 1$ *and a dominant rational map* $f : V_1 \to V_2$ *such that* $f \circ \phi_1 = \phi_2^{(r)} \circ f$. *Then there is a variety* V_0 *and a dominant rational map* $\phi_0 : V_0 \to V_0$, *all defined over* k, *a dominant map* $g : V_2 \to V_0$ *such that* $g \circ \phi_2 = \phi_0 \circ g$, *and* $\deg(\phi_0) = \deg(\phi_2)$.

5. Applications of the CBP to algebraic dynamics

The original result of Matthew Baker. Let k be a field, C a curve over k, and $K = k(C)$. Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be defined over K, and of degree $d \geq 2$. One can define a logarithmic height function on the points of $\mathbb{P}^1(K)$, called the Weil height, and which I will denote by h. For details, please see [1]. If $K = k(t)$, then the Weil height of a point $P \in \mathbb{P}(K)$ is simply the minimal degree of polynomials needed to represent the point P. One then defines the canonical height $\hat{h}(P)$ as:

$$\hat{h}(P) = \lim_{n \to \infty} h(\phi^{(n)}(P))/d^n.$$

[Here $\phi^{(n)}$ denotes the iteration n times of the map ϕ.] One verifies that $\hat{h}(\phi(P)) = d\hat{h}(P)$; moreover, there is a constant $C > 0$, such that for any point P, one has $|\hat{h}(P) - h(P)| < C$. Clearly, any *preperiodic point* P (i.e., such that for some integers $m > n$ one has $\phi^{(m)}(P) = \phi^{(n)}(P)$) must have $\hat{h}(P) = 0$. Baker's theorem shows that these are the only ones, unless, over some finite extension of K one has $(\mathbb{P}^1, \phi) \simeq (\mathbb{P}^1, \psi)$ for some ψ defined over k:

Theorem 5.1 ([1]). *Let* $k \subset K$ *and* ϕ *be as above. Assume that for no finite algebraic extension of* K', *there is an* $M \in \mathrm{PGL}_2(K')$ *such that* $M^{-1}\phi M$ *is defined over* k. *Then a point* $P \in \mathbb{P}^1(K)$ *satisfies* $\hat{h}(P) = 0$ *if and only if it is preperiodic.*

He shows moreover that there is a positive ϵ which bounds below the canonical height of non-preperiodic points of $\mathbb{P}^1(K)$.

5.2. The analogue for higher dimensional varieties. The setting: Let V be a quasi-projective variety defined over K, $\phi : V \to V$ a dominant rational map of degree $d \geq 2$. Once fixed an embedding of V into projective space, the Weil heights of points of $V(K)$ exist as before. (But to obtain the canonical height, additional conditions are necessary.) We assume that for some N, the points $P \in V(K)$ such that all $\phi^{(n)}(P)$, $n \geq 0$, have height $\leq N$, form a Zariski dense subset of V.

The hope: (V, ϕ) is isomorphic to some (W, ψ) defined over k.

5.3. The observation which makes things work. The following observation, due to Szpiro, is what allows model theory to play a role, since it gives a certain configuration which one can exploit.

Given some integer N, the points of $V(K)$ which have Weil height $\leq N$, form what we will call a *limited set*, i.e., there is some algebraic set U defined over k, a constructible map $\pi : U \to V$ (defined over K), such that $\pi(U(k))$ contains all points of $V(K)$ of Weil height $\leq N$, and π is injective on $U(k)$ (see e.g. section 3 of [4]). Consider the following sets:

$$V_0 = \pi(U(k));\ V_n = \bigcap_{0 \leq j \leq n} \phi^{-(j)}(V_0).$$

So, a point P will be in V_n if and only if each of P, $\phi(P), \ldots, \phi^{(n)}(P)$ has Weil height $\leq N$.

The map ϕ induces a (partially defined) constructible map ϕ^* on U. Namely, if $Q \in U(k)$, and $\phi\pi(Q) \in V_0$, then $\phi^*(Q)$ is defined by $\pi\phi^*(Q) = \phi\pi(Q)$. Assume that for the number N above, the sets V_n are Zariski dense in V. We now look at U_n, the Zariski closure of $\pi^{-1}(V_n) \cap U(k)$. These sets form a decreasing chain of Zariski closed infinite subsets of U, which must therefore stabilise at some integer n. Let $\tilde{U} \subset U_n$ be the union of all irreducible components W of U_n such that $\pi(W(k))$ is Zariski dense in V. Then, the constructible ϕ^* induces a permutation of the irreducible components of $\tilde{U}$ of maximal dimension, and for some $r \geq 1$, the constructible map $(\phi^*)^{(r)}$ yields a rational dominant endomap ψ of some irreducible component W of $\tilde{U}$ of maximal dimension. Note that $\pi(W(k))$ is still Zariski dense in V, but that π sends (W, ψ) to $(V, \phi^{(r)})$. It turns out that this is sufficient to obtain some results, using Theorem 4.12.

Theorem 5.4 ([5, 3.2], [2, 4.12]). *With assumption as in 5.2, let $\mathcal{U}$ be a model of ACFA containing K, and a a generic point of V over K satisfying $\sigma(a) = \phi(a)$.*

(1) *Assume that the semi-minimal analysis of $tp(a/K)$ does not involve* $\mathrm{Fix}(\sigma)$. *Then there is a bijective morphism $g : (V, \phi) \to (V_0, \phi_0)$ for some (V_0, ϕ_0) defined over k. In characteristic* 0*, this g is a birational isomorphism.*

(2) *In the general case, there is a dominant rational map $(V, \phi) \to (V, \phi_0)$ where (V, ϕ_0) is defined over k, and* $\deg(\phi) = \deg(\phi_0)$.

Sketch of Proof. I will use (the proof of) 4.11 in [2], and follow its notation. By the above discussion 5.3, we know that there is some algebraic dynamics (V_1, ϕ_1) defined over k, and which dominates $(V, \phi^{(r)})$ for some $r \geq 1$. Let $\mathcal{U}$ be a model of ACFA containing K, let a_2 be a generic of V satisfying $\sigma(a_2) = \phi(a_2)$. Applying 4.11 of [2] (with $K_1 = k$, $K_2 = K$ and $(V_2, \phi_2) = (V, \phi)$), there is $a_3 \in K(a_2)$ such that $\sigma(a_3) \in k(a_3)$. If V_0 is the algebraic locus of a_3 over k, and $\phi_0 \in k(V_0)$ is such that $\phi_0(a_3) = \sigma(a_3)$, then $\deg(\phi) = \deg(\phi_0)$, and there is a rational dominant map $(V, \phi) \to (V_0, \phi_0)$. This gives (2).

The proof of 4.11 in [2] shows that $tp(a_2/K(a_3)_{\sigma^{\pm 1}})$ is almost-internal to $\mathrm{Fix}(\sigma)$. Hence, in case (1), it must be algebraic. Thus $K(a_2)$ is a finite algebraic extension of $K(a_3)$. Let $\alpha \in K(a_2)$ be defined by $K(\alpha) = K(a_2) \cap K(a_3)^s$, so that $K(a_2)/K(\alpha)$ is purely inseparable.

Now, recall from the proof of 4.11 that there is some generic a_1 of V_1 over K, such that $a_2 \in K(a_1)$. Then $k(a_1)$ and $K(a_3)$ are linearly disjoint over $k(a_3)$, and because $K(\alpha)/K(a_3)$ is separable and $K(a_2) \subset K(a_1)$, it follows that $K(\alpha) = K(\beta)$ for some $\beta \in k(a_1)$. Then $\beta \in k(a_3)^s$. As $\sigma(a_2) \in K(a_2)$, we have $\sigma(\alpha) \in K(\alpha)$, hence $\sigma(\beta) \in k(\beta)$. Let $\tilde{V}$ be the algebraic locus of β over k, and $\tilde{\phi} \in k(\tilde{V})$ such that $\sigma(\beta) = \tilde{\phi}(\beta)$, g the rational map $V \to \tilde{V}$ such that $g(a_2) = \beta$. Then g is generically bijective, and sends (V, ϕ) to $(\tilde{V}, \tilde{\phi})$. In characteristic 0, we may take $\alpha = a_2$, and g is then birational. This finishes the proof of (1). □

5.5. Comments. The fact that we work with function fields only tells us about the generic behaviour of the algebraic dynamics, and does not allow us to show full isomorphisms, only birational isomorphisms.

Remark 5.6. If in addition to the hypotheses of 5.2, one assumes that the map ϕ is a polarised morphism with associated constant $q > 1$, then the conclusion of 5.4(1) holds, so that we get the full result. This follows from an observation made without proof in [4]. The proof I sketch below is due to Hrushovski.

Proof. First, note that the hypotheses imply, by a result of Fakhruddin [8], that we may assume that $V \subset \mathbb{P}^N$ for some N, and that the morphism ϕ on V is the restriction to V of a morphism $\psi : \mathbb{P}^N \to \mathbb{P}^N$. Suppose that the conclusion of 5.4(1) does not hold, and let $\mathcal{U}$ be a model of ACFA containing K.

Let $g : (V, \phi) \to (V_0, \phi_0)$ be given by 5.4, with $\deg(\phi) = \deg(\phi_0)$, let $a = a_2 \in \mathcal{U}$ be a generic of V satisfying $\sigma(a_2) = \phi(a_2)$ and let $a_3 = g(a_2)$ (a generic of V_0 satisfying $\sigma(a_3) = \phi_0(a_3)$). Equality of the degrees of ϕ and ϕ_0 implies that the restriction of ϕ to $S = g^{-1}(a_3)$ is an isomorphism. The variety $S' = \phi(S)$ equals S^σ, and therefore $\deg(S') = \deg(S)$. We will show the following:

If S is a subvariety of V, and $\deg(S) = \deg(\phi(S))$ (as subvarieties of $\mathbb{P}^N$), then the degree of the map ϕ restricted to S is $q^{\dim(S)}$.

Let $r = \dim(S)$, and let $L_1, \dots, L_r$ be generic hyperplanes. Then $\deg(S') = S' \cdot L_1 \cdot \dots \cdot L_r$, and also equals $|S' \cap L_1 \cap \dots \cap L_r|$, the number of points of $S' \cap L_1 \cap \dots \cap L_r$ counted with multiplicities. Pulling back by ϕ, we get

$$\begin{aligned} \deg(S) = \deg(S') \deg(\phi|S) &= |\phi^{-1}(S') \cap \phi^{-1}(L_1) \cap \dots \cap \phi^{-1}(L_r)| \\ &= S \cdot qL_1 \cdots qL_r = q^r \deg(S) \end{aligned}$$

(here we use $\phi^* L_i = qL_i$). As $\deg(S) = \deg(S')$, the restriction of ϕ to S has degree q^r.

As $\phi|S$ is birational and therefore of degree 1, we must have $r = 0$. This implies that S is finite, i.e., that a_2 is algebraic over $K(a_3)$, and we conclude as in 5.4(1). □

Acknowledements. The author thanks MSRI for its support during the spring 2014.

References

[1] Matthew Baker, *A finiteness theorem for canonical heights attached to rational maps over function fields*, J. Reine Angew. Math. **626** (2009), 205–233.

[2] Z. Chatzidakis, *A note on canonical bases and one-based types in supersimple theories*, Confluentes Mathematici Vol. 4, No. 3 (2012) 1250004 (34 pages). DOI: 10.1142/S1793744212500041.

[3] Z. Chatzidakis and E. Hrushovski, *Model theory of difference fields*, Trans. Amer. Math. Soc. **351** (1999), 2997–3071.

[4] ______, *Difference fields and descent in algebraic dynamics, I*, Journal of the IMJ, **7** (2008) No 4, 653–686.

[5] ______, *Difference fields and descent in algebraic dynamics, II*, Journal of the IMJ, **7** (2008) No 4, 687–704.

[6] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, *Model theory of difference fields, II: Periodic ideals and the trichotomy in all characteristics*, Proceedings of the London Math. Society (3) **85** (2002), 257–311.

[7] R.M. Cohn, *Difference algebra*, Tracts in Mathematics **17**, Interscience Pub. 1965.

[8] Najmuddin Fakhruddin, *Questions on self maps of algebraic varieties*, J. Ramanujan Math. Soc. **18** (2003), no. 2, 109–122.

[9] E. Hrushovski, *The Manin-Mumford conjecture and the model theory of difference fields*, Ann. Pure Appl. Logic **112** (2001), no. 1, 43–115.

[10] Ehud Hrushovski, Daniel Palacin, and Anand Pillay, *On the canonical base property*, preprint 2012. arXiv:1205.5981.

[11] E. Hrushovski and A. Pillay, *Weakly normal groups*, in: Logic Colloquium **85**, North Holland 1987, 233–244.

[12] A. Macintyre, *Generic automorphisms of fields*, APAL **88** Nr 2-3 (1997), 165–180.

[13] Rahim Moosa, *On saturation and the model theory of compact Kähler manifolds*, J. Reine Angew. Math. **586** (2005), 1–20.

[14] R. Moosa and A. Pillay, *On canonical bases and internality criteria*, vol. **52** no. 3 (2008), 901–917.

[15] Anand Pillay, *Model-theoretic consequences of a theorem of Campana and Fujiki*, Fundamenta Mathematicae, **174**, (2002), 187–192.

[16] A. Pillay and M. Ziegler, *Jet spaces of varieties over differential and difference fields*, Selecta Math. (N.S.) **9** (2003), no. 4, 579–599.

[17] T. Scanlon, *p-adic distance from torsion points of semi-abelian varieties*, J. für Reine u. Ang. Mat. **499** (1998), 225–236.

[18] ———, *The conjecture of Tate and Voloch on p-adic proximity to torsion*, International Mathematics Research Notices, 1999, no. 17, 909–914.

[19] ———, *Diophantine geometry of the torsion of a Drinfeld module*, J. Number Theory **97** (2002), no. 1, 10–25.

[20] F. Wagner, *Simple theories*, Kluwer Academic Pub., Dordrecht 2000.

UFR de Mathématiques, UMR 7586,Université Paris 7, Case 7012, 75205 Paris cedex 13, France
E-mail: zoe@math.univ-paris-diderot.fr